CLAIMS

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations; and

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, wherein said one of the cryptographic operations comprises:

indicating whether said one of the cryptographic operations has been interrupted by an interrupting event.

2. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

3. The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

4. The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

5. The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

6. The apparatus as recited in claim 5, wherein said block cipher mode comprises electronic code book (ECB) mode.

7. The apparatus as recited in claim 5, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

8. The apparatus as recited in claim 5, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

9. The apparatus as recited in claim 5, wherein said block cipher mode comprises output feedback (OFB) mode.

10. The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes that said one of the cryptographic operations be accomplished on a plurality of text blocks.

11. The apparatus as recited in claim 10, further comprising:

a bit, coupled to said execution logic, configured to indicate whether said one of the cryptographic operations has been interrupted by an interrupting event.

12. The apparatus as recited in claim 11, wherein said bit is contained within a flags register.

13. The apparatus as recited in claim 12, wherein said flags register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

14. The apparatus as recited in claim 1, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input data block is interrupted.

15. The apparatus as recited in claim 14, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input data block.

16. The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify pointers to input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block.

17. The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

18. The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

19. The apparatus as recited in claim 1, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

20. The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

21. The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

22. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

23. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

24. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

25. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

26. The apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key.

27. The apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key schedule.

28. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

29. The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

30. The apparatus as recited in claim 1, wherein said execution logic comprises:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

31. An apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations; and

a bit within a register, operatively coupled to said cryptography unit, configured to indicate that execution of said one of the cryptographic operations has been interrupted by an interrupting event.

32. The apparatus as recited in claim 31, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

33. The apparatus as recited in claim 31, wherein said register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

34. The apparatus as recited in claim 31, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input data block is interrupted.

35. The apparatus as recited in claim 34, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input data block.

36. The apparatus as recited in claim 31, further comprising:

block pointer logic, operatively coupled to said cryptography unit, configured to direct said computing device to modify pointers to input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block.

37. The apparatus as recited in claim 31, further comprising:

block pointer logic, operatively coupled to said cryptography unit, configured to direct said computing device to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

38. The apparatus as recited in claim 31, further comprising:

block pointer logic, operatively coupled to said cryptography unit, configured to direct said computing device to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

39. The apparatus as recited in claim 31, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

40. A method for performing cryptographic operations in a device, the method comprising:

executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction prescribes the one of the cryptographic operations; and

indicating whether an interrupting event has occurred during said executing.

41. The method as recited in claim 40, wherein said indicating comprises pointing out whether an interrupt, an exception, a page fault, or a task switch has occurred during said executing.

42. The method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in a register within the device.

43. The method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in an EFLAGS register within an x86-compatible microprocessor.

44. The method as recited in claim 40, further comprising:

transferring program control to a program flow configured to process the interrupting event, and interrupting said executing of the one of the cryptographic operations on a current input data block.

45. The method as recited in claim 44, further comprising:

upon return of program control to said cryptographic instruction following said transferring, performing said executing on said current input data block.

46. The method as recited in claim 40, further comprising:

directing the device to modify pointers to input and output data blocks in memory to point to next input and output data blocks at the completion of the one of the cryptographic operations on a current input data block.

47. The apparatus as recited in claim 40, further comprising:

directing the device to modify contents of a block counter register to indicate that the one of the cryptographic operations has been completed on a current input data block.

48. The apparatus as recited in claim 40, further comprising:

directing the device to preserve or to generate and preserve data resulting from performance of the one of the cryptographic operations on a current block of data such that, upon return from the interrupting event, performance of the one of the cryptographic operations can continue with a following block of data.

49. The apparatus as recited in claim 40, wherein said receiving comprises:

Prescribing the cryptographic instruction according to the x86 instruction format.

50. The method as recited in claim 40, wherein said receiving comprises:

prescribing an encryption operation as the one of the cryptographic operations, wherein the encryption operation comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

51. The method as recited in claim 40, wherein said receiving comprises:

prescribing a decryption operation as the one of the cryptographic operations, wherein the decryption operation comprises decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

52. The method as recited in claim 40, wherein said executing comprises:

accomplishing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

53. The method as recited in claim 40, wherein said receiving comprises:

specifying, within the cryptographic instruction, a block cipher mode to be employed in accomplishing the one of the cryptographic operations.

54. The method as recited in claim 53, wherein the block cipher mode comprises electronic code book (ECB) mode.

55. The method as recited in claim 53, wherein the block cipher mode comprises cipher block chaining (CBC) mode.

56. The method as recited in claim 53, wherein the block cipher mode comprises cipher feedback mode (CFB) mode.

57. The method as recited in claim 53, wherein the block cipher mode comprises output feedback (OFB) mode.